



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



020.301 CHFS Network User Accounts

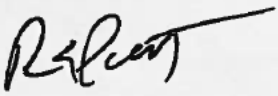

**Version 2.2
November 6, 2017**

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS OATS Policy Charter Team
11/6/2017	2.2	Revision Date	CHFS OATS Policy Charter Team
11/6/2017	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	11/6/2017	ROBERT E. PUTT	
CHFS Chief Security Officer (or designee)	11/6/2017	DENNIS E. LEBER	

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

Table of Contents

020.301 CHFS NETWORK USER ACCOUNTS	4
1 POLICY OVERVIEW.....	4
1.1 PURPOSE	4
1.2 SCOPE	4
1.3 MANAGEMENT COMMITMENT.....	4
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	4
1.5 COMPLIANCE	5
2 ROLES AND RESPONSIBILITIES	5
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	5
2.2 SECURITY/PRIVACY LEAD	5
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	5
2.4 CHFS STAFF AND CONTRACTOR EMPLOYEES	6
2.5 SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	6
2.6 KENTUCKY ONLINE GATEWAY (KOG) ENTERPRISE IDENTITY MANAGEMENT (EIM) ADMINISTRATORS	6
2.7 SERVICE REQUESTOR	6
3 POLICY REQUIREMENTS	6
3.1 GENERAL INFORMATION	6
3.2 DOMAIN ACCOUNT CREATION	7
3.3 APPLICATION ACCESS.....	7
3.4 NETWORK ACCESS.....	7
3.5 REMOVAL/DELETION OF ACCESS.....	8
3.6 EXTERNAL AUDITOR ACCESS	8
3.7 OFF SHORE ACCESS	8
4 POLICY DEFINITIONS.....	8
5 POLICY MAINTENANCE RESPONSIBILITY	9
6 POLICY EXCEPTIONS	9
7 POLICY REVIEW CYCLE.....	9
8 POLICY REFERENCES	10

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

020.301 CHFS Network User Accounts

Category: 020.300 Administrative Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through an incident response and reporting policy. This document establishes the agency's Network User Accounts Policy, to manage risks and provide guidelines for security best practices regarding network accounts and access.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) to request an exception to this policy.

CHFS's long term goal is to configure all cabinet applications within the Kentucky Online Gateway (KOG), until that time only applicable agencies whose applications are currently configured through KOG are mandated to comply with this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and CHFS Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of this policy along with the CHFS OATS Information Security (IS) Team.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS IS Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position will be responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notification in accordance with HIPAA rules and regulations.

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead roles to work with the application's development team to document components that are not included in the base server build and ensure backups are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

2.6 Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) Administrators

Authorized KOG personnel are responsible for taking electronically submitted service requests received by KOG and submitting them to the Commonwealth Service Desk for completion. These authorized staff personnel are responsible for basic validation of service request information and are listed as an approved IT service contact to submit service desk tickets for CHFS.

2.7 Service Requestor

A CHFS division director approved and appointed designated individual(s) to submit service requests through KOG (i.e. Active Directory (AD), Virtual Private Network (VPN), Home Folder, Shared Folder, Telephone, Enhanced Mailbox, Account, Skype for Business, Other). These designated personnel validate all KOG required user and billing code information is obtained from the CHFS personnel requesting services.

3 Policy Requirements

3.1 General Information

CHFS adheres to Commonwealth Office of Technology (COT) Enterprise Policy: CIO-072- Identity and Access Management Policy. Maintenance of CHFS Domain accounts is coordinated through COT.

The immediate supervisor of a new employee is responsible for ensuring the employee reads and agrees with all information provided through the Office of Human Resource Management (OHRM) Personnel Handbook. CHFS employees must read, understand, and sign the CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219) upon initial hire and annually thereafter.

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

The immediate supervisor, or designee, is responsible for requesting that an employee's CHFS Domain account be created, modified, or deleted, as needed, through the Kentucky Online Gateway (KOG).

CHFS staff must coordinate with the CHFS KOG team to obtain mainframe user account access. Through KOG, via the Enterprise Information Management Solution (EIM), the designated requestor for the user's department shall submit a request for mainframe access and must obtain a CHFS-219B form from the user prior to access to mainframe access being fulfilled.

3.2 Domain Account Creation

Newly hired/on boarded state staff are entered into the Human Resource (HR) KHRIS system. Once actions are approved and completed in KHRIS employee data is automatically sent to EIM and the domain account is created. This information is then synced to KOG.

Newly hired/on boarded contract/vendor staff work with the agency/division's service requestor for a request to create a domain account through KOG. Once KOG receives the request the KOG Administrators manually retain and feed the data into EIM. Once KOG Administrators complete the process the contract/vendor staff's domain account is created.

3.3 Application Access

State and contract/vendor staff requesting application access work with the agency/division's service requestor to submit a request via KOG. The request for the requested application is entered through KOG's Request Application Portal by the Service Requestor for completion. At this point the request is routed through an automated workflow for approval.

3.4 Network Access

After a state or contract/vendor's account has been created, and if deemed necessary, access to network resources (i.e. database access, server access, etc.) may be requested by appropriate management. The following COT forms must be filled out:

- F181- Staff Service Request Form
- F085- Security Exemption Form

When production data/access is being requested, the request forms must be submitted and approved to the OATS IS management for approval.

Once completed and CHFS approved, submit the forms to the CHFS Authorized Agency's IT Services Contact, they will review and send to the Commonwealth Service Desk for processing. Please refer to the COT Forms Page for instructions and additional detailed information.

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

3.5 Removal/Deletion of Access

For state staff, accounts are removed from EIM once KHRIS actions within HR are completed. Once actions are approved and completed in KHRIS employee data is automatically sent to EIM and synced to KOG for removal. Once information is fed into KOG, the KOG account is marked as inactive.

For contract/vendor staff, accounts to be removed/deleted are requested within the KOG the KOG Administrators manually retain and fed the removal request data into EIM. Once KOG Administrators complete the process the contract/vendor staff's domain account is marked as inactive.

3.6 External Auditor Access

All vendors/auditors must be approved, have business justification and/or agreements in place with the appropriate CHFS agencies to obtain application or network access. Only vendors/auditors deemed appropriate will be approved for minimum necessary access for a defined duration of time. Vendors/auditors are bound by CHFS usage policies and procedures as well as all other federal rules and regulations. Form, CHFS-219V must be filled out and completed along with up-to-date antivirus software. External vendor access to any KOG application must follow the steps outlined in the CHFS External Auditor Access Request Procedure.

3.7 Off Shore Access

Production data is prohibited to be accessed by personnel located off-shore. All users requesting production data must be located within the United States. This applies to all CHFS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. By definition, production data is classified as "production data" when located in any environment. If production data is obfuscated, it is then not considered live production data.

4 Policy Definitions

- **Agency:** for the purpose of this document, agency or agencies refers to any department under the Cabinet of CHFS.
- **Confidential Data:** as defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to: data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Enterprise Identity Management (EIM):** identity management solution used to provide internal users with network service entitlements.
- **Network Access:** access to servers, Active Directory, databases, folders, within or on the CHFS boundaries.

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

- **Obfuscated Data:** data masked or the process of hiding original data within random characters or data sets.
- **Production Data:** data within the system that contains citizens personal, identifiable, sensitive, and confidential information. This data is classified as production data if found in any environment and not obfuscated.
- **Sensitive Data:** as defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples would include, but are not limited to information identifiable to an individual (i.e. date of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) as well as Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

For any staff located within the Department for Behavioral Health, Development, and Intellectual Disabilities (BHDID) who have not yet been on boarded or utilize KOG, the COT F181EZ form must be used to request any action (create, modify, or delete) related to CHFS domain accounts/access.

Once forms are completed and required management approval is received, the Agency's IT Services Contact can then submit the access request forms to the Commonwealth Service Desk for (CommonwealthServiceDesk@ky.gov) for completion. Please refer to the COT Forms Page (<http://technology.ky.gov/Pages/cotForms.aspx>) for instructions and more detailed information. For Agency approved contact listing please click here: <https://gotsource.ky.gov/docushare/dsweb/Get/Document-391539/>.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

020.301 CHFS Network User Accounts	Current Version: 2.2
020.300 Administrative Security	Review Date: 11/06/2017

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS External Auditor Access Request Procedure
- CHFS External Auditor Access Request Form
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219)
- Enterprise IT Policy: CIO-072- Identity and Access Management Policy
- Enterprise IT Form Instructions: F181EZ- Staff Service Request, EZ Version, Form Instructions
- Enterprise IT Form: F181EZ- Staff Service Request, EZ Version, Form
- Enterprise IT Form Instructions: F181i- Staff Services Request Form Instructions
- Enterprise IT Form: F181- Staff Service Request Form (and COT Entrance/Exit Form)
- Enterprise IT Form: F085- Security Exemption Request Form
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- National Institute of Standards and Technology (NIST) Special Publication 800-12 Revision 1, Introduction to Information Security (Draft)
- National institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National institute of Standards and Technology (NIST) Special Publication 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- Office of Human Resource Management (OHRM) Personnel Handbook
- Social Security Administration (SSA) Security Information